anand guru

SOC EXPERTS

Interview Questions on
Correlation Rules (Use Cases)

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

What is Correlation?

Correlation is the process of identifying a suspicious activity by defining set of conditions.

Example: **A user account created during non-business hours**

Here there is a correlation between two (2) conditions.

- A event – User account created
- Time Condition – During non-business hours (Between 7pm and 7am)

How do you categorize correlation rules?

Different organization categorize correlation rules in different ways. Few of them are

Based on Device – Firewall based rules, AV based rules, Proxy based rules etc.

Based on Category – Malware, Access, Network, Database etc.

According to the phases of Cyber Kill Chain – Rule to detect Reconnaissance Phase or Exploit Phase etc.

anand guru

What is a cross-platform correlation rule?

A correlation rule that involves at least two (2) different log source is called a cross-platform correlation rule.

Example 1: **High severity IPS alert for a Vulnerable host**

Here we are correlating an event from IPS plus we are using the data from the Vulnerability Assessment log source

Example 2: **Multiple RDPs after VPN access**

Here we are correlating events from Firewall (for VPN access) and any server based on an authentication event.

Malware Use cases.

Sl. No.	Use case	Description	Pre-requisites	Detection logic
1	**Malware detection on a Server**	If there is a malware detection on a server, it is definitely worth taking a look at irrespective of the AV action.	Create a List in SIEM of all the servers	Category=Malware Host (belongs to) Server List
2	**Unhandled Malware**	This is when the AV detects the malware but is unable to clean, delete or quarantine	None	Category = Malware Action = Delete failed OR Quarantine failed or Clean Failed
3	**Same Malware on Multiple Host**	Indicates several users are targeted via an email or a commonly used website	None	Category= Malware No. of Unique host = 5 Time Windows = 1 hour Malware Name is constant (group by)
4	**Multiple Malware Infection on a Host**	Indicates either the user is trying to download or copy a malicious file over and over again. OR a malware is partially executed and trying to perform a activity that is being detected as malicious by AV	None	Category = Malware No. of Event = 5 Time Window = 1 hours Host should be constant (group by)
5	**Outbound Communication to Blacklisted IP** OR **Possible Botnet Activity Detected**	A compromised host is initiating communication to its Command & Control	Create a List in SIEM of all Blacklisted IPs. This is done through Threat intelligence integration	Log Source = Firewall Direction = Local2Remote Destination IP (belong to) Blacklisted IP List
6	**Too Many DNS Lookup Failures**	Indicates the presence of Domain Generating Algorithm. DGAs are used by malware authors to avoid detections from Threat Intelligence.	None	Log Source = DNS DNS Response =NXDOMAIN No. of Event = 1000 Client is constant
7	**High Resource (CPU or Memory) Utilization**	High resource consumption is an indication of malware activity	Install an agent on the servers that will provide the resource utilization data	Avg. Memory Consumption for 10 minutes > 90% OR Avg. CPU Utilization for 10 minutes > 90%
8	**Unauthorized Process Detected**	A new (unknown) process is running in a server	Install Sysmon to collect process related information. Make a list of all authorized processes	Event = New Process Started Process Name (Doesn't belong to) Authorized Processes List

Use Cases on Firewall.

Sl. No.	Use case	Description	Pre-requisites	Detection logic
1	**Too many firewall Denies for same Source**	If an attacker is trying to connect over and over again and is being blocked. OR a malware is trying to connect to C&C and it is being denied	None	Event Type = Connection Denied No. of Events = 300 Time Window = 5 minutes With Source IP constant
2	**VPN logins from Multiple geolocations**	A user cannot connect to VPN from 2 geo-location	None	Event Type = VPN Authentication Unique Geolocations = 2 With Username held constant
3	**Horizontal Scan detected**	When a attacker tries to scan the available IPs as part of information gathering	None	Log Source = Firewall Unique Destination IPs = 10 Time Window = 1 minute With same Source IP
4	**Vertical Scan detected**	When a attacker tries to scan the available ports on a server as part of information gathering	None	Log Source = Firewall Unique Destination Ports = 100 Time Window = 1 minute With same Source IP and Destination IP
5	**Scanning on Remote Access Ports**	When an attacker tries to connect to company server on remote access ports	Create a List of all Remote Access ports like 3389, 22, 21, 1433, 3306 etc.	Log Source = Firewall Destination Port = List of Remote Access Ports No. of Event = 20 Time Window = 30 minute With same Destination IP
6	**High Volume of connection from country of concern**	Countries the company doesn't do business with or if the relationship of the country is not good with home country	List of all countries of concern	Log Source = Firewall Source Country = List of Countries of concern
8	**Outbound SMTP traffic from Unauthorized Host**	An infected machine might start sending spam email from inside the company.	List of all email servers	Log Source=Firewall Source IP != List of Email Server Destination Port = 25
9	**Proxy Bypass Attempt**	If any client or server tries to connect to internet directly (Usually done by users trying to do things that are not allowed. OR it could be a malware trying to connect to C&C	None	

Use Cases on AD and Windows Logs.

Sl. No.	Use case	Description	Pre-requisites	Detection logic
1	**Local account created**	User account created on server (not AD)	None	Event ID = 4720 Log Source != AD
2	**User added/removed to admin group**	Helps in monitoring accidental or attacker privilege escalations	Create a list of High Privileged Groups	Event ID = Group = List of High Privileged Groups
3	**Too many account lockouts**	Bruteforce is happening on several accounts	None	Event ID = 4740 No. of Events >10 Time Window = 1 hour
4	**Service Account Password Reset**	Service accounts are very sensitive as they have higher privileges and do not get locked out	List of all service accounts	Event ID = 4724 User in List fo Service Accounts
5	**AD Group Created/Deleted**	Groups are not created very often, so it is good to monitor group creations and deletions in AD	None	Event ID = 4731, 4727 for created Event ID = 4734, 4730 for deleted
6	**Domain Account Creation During Non-Business Hours**	Suspicious activity, Account created by Attacker	None	Event ID = 4720 Time (Not in) Monday – Friday 7am to 7pm
7	**Too many password resets**	Suspicious activity	None	Event ID = 4724 No. of Event > 10 Time window = 1 hour
8	**Audit Logs Cleared**	Attacker or a Admin is clearing the tracks	None	Event ID = 1102

Correlation Rules based on Cyber Kill Chain

Phase	Use case
Reconnaissance	• **Horizontal Scan detected** • **Vertical Scan detected** • **Directory Traversal (alerted by WAF)** • **High Volume of connection from country of concern**
Weaponization	• This phase cannot be detected as it is done by the attacker at his side.
Delivery	• **Too many email from same domain** • **Too many email with same Subject line** • **Email with multiple attachments** • **Visit to malicious website**
Exploit	• **Too many file modifications** • **Registry changes detected**
Install	• **High Resource Utilization** • **New Process detected**
Command & Control	• **Communication to Bad reputation IP** • **Too many DNS Lookup failures**
Actions on Objective	• **File modification** • **High volume of data outbound** • **Critical Server Shutdown**

anand guru

How do you detect malware in the network without AV?

Behavior based malware detection.

- Outbound Communication to Blacklisted IP OR Possible Botnet Activity Detected
- Too Many DNS Lookup Failures (Indicates possible DGA running in the network)
- High Resource (CPU or Memory) Utilization
- Unauthorized Process Detected

anand guru

How do you detect SQL Injection in SIEM?

We can write correlation to trigger on.

- SQLi related alert from IPS or WAF
- Unusual Username (User name with special characters used)
- Too many errors on Database
- Too many SELECT statements
- DROP command executed

These rules are typically run on **Database Audit Logs**

How do you detect Ransomware using SIEM?

We can write correlation to trigger on.

- Behavioral analysis for detecting user privilege escalation
- High Volume of administrator's logins.
- Monitoring of traffic parameters deviation from their baseline characteristics.
- Communication with malicious IP addresses, URLs, domains, and suspicious geographic destinations, as well as a traffic volume surge may indicate ransomware presence in a network.
- File Modifications (if we have File Integrity Monitoring events)

anand guru

Correlation Rule to detect Phishing Email.

We can write correlation to trigger on.

- Too many email from same domain
- Too many email with same Subject line
- Email from Blacklisted IP
- Email with multiple attachments
- Email blocked due to phishing link (Email gateway events)
- Communication to Bad URL

anand guru